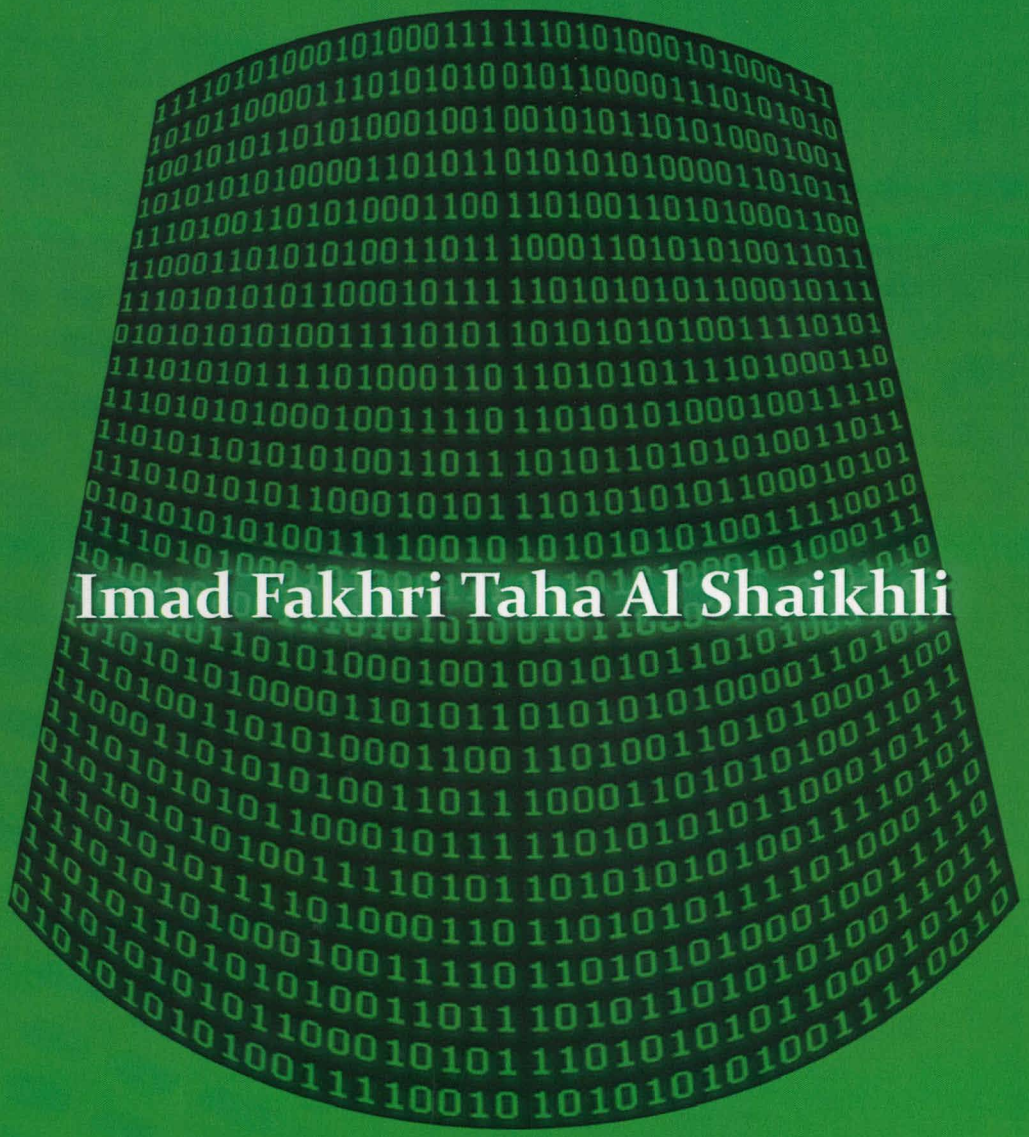
Cryptography

Past, Present and Future

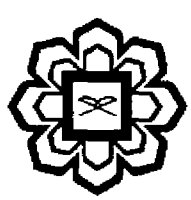


Imad Fakhri Taha Al Shaikhli

IIUM PRESS
INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

Cryptography: Past, Present and Future

Imad Fakhri Taha Al Shaikhli



IIUM Press

Published by:

IIUM Press

International Islamic University Malaysia

First Edition, 2011

Perpustakaan Negara Malaysia Cataloguing-in-Publication Data

Imad Fakhri Taha Al-Shaikhli
Cryptography: Past, Present and Future
Imad Fakhri Taha Al-Shaikhli

ISBN: 978-967-418-091-1

Member of Majlis Penerbitan Ilmiah Malaysia – MAPIM
(Malaysian Scholarly Publishing Council)

Printed by :
IIUM PRINTING SDN. BHD.
No. 1, Jalan Industri Batu Caves 1/3
Taman Perindustrian Batu Caves
Batu Caves Centre Point
68100 Batu Caves
Selangor Darul Ehsan

TABLE OF CONTENTS

- Sibomana Hilali Hussein

10. Message Digest (MDx) Family

- Imad Fakhri Taha Al Shaikhli
- Sufyan Salim Mahmood Al Dabbagh
- Khanssaa Munthir Abdulmajed
- Ahmad Faridi Abdul Matin
- Sibomana Hilali Hussein

ABSTRACT

In this article we will talk about the description of Message Digest (MDx) Family. Also we will introduce into Message Digest 2 (MD2), Message Digest 4 and 5 (MD4 and MD5). Moreover, we will describe the Security of the MDx family hash function.

DESCRIPTION

According to the IETF's memorandum in regards to MD2, MD4 and MD5, all of these algorithms take as input a message of arbitrary length and produce as output a 128-bit (16 bytes) message digest of the input. These algorithms were intended for digital signature applications where a message needs to be compressed securely before being signed with a private key under the public key cryptography such as the RSA. Despite their apparent similarities they are different in many ways. (Kaliski, 1992; Rivest, 1992)

Essentially, MD2, MD4 and MD5 all use the same mechanism. The message is divided into blocks of certain size (depending on which message digest is in use). Each block will then be processed with a compression function (see Figure 10.1). (Robshaw, 1996)